THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

WINSTON FERNANDEZ, *on behalf of himself and all others similarly situated*, Plaintiff, v. AUS, Inc., Defendant.	Case No. _____ **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Winston Fernandez ("Plaintiff") brings this Class Action Complaint against AUS, Inc. ("AUS" or "Defendant"), as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels' investigations, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiff brings this class action against AUS to seek damages for Plaintiff and the class of consumers and current or former employees of AUS who he seeks to represent, as well as other equitable relief, including, without limitation, injunctive relief designed to protect the very sensitive information of Plaintiff, other consumers, and current or former AUS employees. This action arises from

AUS's failure to properly secure and safeguard personal identifiable information, including without limitation, the full names and Social Security numbers (collectively, "Sensitive Information" or "PII").

2. AUS is a company primarily providing consulting and market research services to its clients, but also providing other business management related products and services through its subsidiaries – SSRS, MSG, RoyaltySource, and AUS Consultants.

3. As part of its services, AUS requires that its customers, including Plaintiff and Class Members, provide AUS with their PII, including their full names and Social Security numbers.

4. Beginning on or about January 4, 2023, AUS notified state Attorneys General and/or many of its customers about a widespread data breach involving sensitive PII of thousands of individuals, including customers and current or former employees.[1] As an example, the Massachusetts Attorney General has posted to its website a draft letter from AUS President and CEO John L Ringwood notifying residents of the Data Breach.[2] In its Notice Letter, AUS explained that its investigation concluded on December 23, 2022. According to the letter, the investigation uncovered that AUS experienced a ransomware attack on November

[1] Ex. 1, January 4, 2023, Winston M. Cuevas Fernandez Data Breach Notice Letter ("Data Breach Notice Letter")

[2] https://www.mass.gov/doc/assigned-data-breach-number-28853-aus-inc/download (last accessed Mar. 23, 2023)

28, 2022 that resulted in network disruption. To date, though, AUS cannot confirm what specific information was affected for each individual whose information was compromised.[3]

5. The full extent of the types of sensitive personal information, the scope of the breach, and the root cause of the Data Breach is all within the exclusive control of Defendant and its agents, counsel, and forensic security vendors at this phase of litigation.

6. Defendant had numerous statutory, regulatory, contractual, and common law duties and obligations, including those based on its affirmative representations to Plaintiff and Class Members, to keep their PII confidential, safe, secure, and protected from unauthorized disclosure or access.

7. Moreover, by obtaining, collecting, using, and deriving benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties to those persons, and knew or should have known that it was responsible for safeguarding and protecting Plaintiff's and Class Members' PII from unauthorized disclosure or criminal hacking activity.

8. In acquiring and maintaining Plaintiff's and Class Members' Sensitive Information, Defendant expressly and impliedly promised to safeguard Plaintiff's and Class Members' PII.

9. Plaintiff and Class Members reasonably expected and relied upon

[3] Data Breach Notice Letter

Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

10. Plaintiff and Class Members would not have paid the amounts they paid for Defendant's services, had they known their information would be maintained using inadequate data security systems. Defendant, however, breached their duties, promises, and obligations, and Defendants' failures increased the risk that Plaintiff's Sensitive Information would be compromised in the event of a likely cyberattack.

11. Upon information and belief, Defendant is responsible for allowing this Data Breach because of multiple acts of negligence, including but not limited to its: failure to design, implement, and maintain reasonable data security systems and safeguards; and/or failure to exercise reasonable care in the hiring, supervision, and training of its employees and agents and vendors; and/or failure to comply with industry-standard data security practices; and/or failure to comply with federal and state laws and regulations that govern data security and privacy practices and are intended to protect the type of Sensitive Information at issue in this action.

12. Upon information and belief, despite its role in managing so much Sensitive Information, Defendant failed to take basic security measures such as encrypting its data or following industry security standards. Moreover, Defendant failed to recognize and detect that unauthorized third parties had accessed its

network. Defendant further failed to recognize that substantial amounts of data had been compromised, and more likely than not, exfiltrated and stolen. Had Defendant not committed the acts of negligence described herein, it would have discovered the Data Breach sooner – and/or prevented the invasion and theft altogether.

13. In this era of frequent data security attacks and data breaches, particularly in the financial industry, Defendant's failures leading to the Data Breach are particularly egregious, as this Data Breach was highly foreseeable.

14. And as a result of Defendant's failures to protect the PII of Plaintiff and Class Members the PII was compromised and accessed. Upon information and belief, their Sensitive Information was likely downloaded, and/or exfiltrated by malicious cyber criminals, who targeted that information through their wrongdoing.

15. Criminal hackers obtained Plaintiff's and Class Members' PII because of its value in exploiting and stealing the identities of Plaintiff and Class Members.

16. As a direct and proximate result of the Data Breach, Plaintiff and the Class Members are now at a significant present and future risk of identity theft, financial fraud and/or other identity-theft or fraud, imminently and for years to come.

17. In the months and years following the Data Breach, Plaintiff and the other Class Members will experience numerous types of harms as a result of Defendant's ineffective and inadequate data security measures. Some of these harms will likely include fraudulent charges on financial accounts, opening

fraudulent financial accounts, and targeted advertising without patient consent.

18. Plaintiff and Class Members have also now lost the economic value of their Sensitive Information. Indeed, there is both a healthy black market and a legitimate market for that PII. Just as Plaintiff's and Class Members' PII were stolen, *inter alia*, because of its inherent value in the black market, the inherent value of Plaintiffs' and the Class Members' Sensitive Information in the legitimate market is now significantly and materially decreased.

19. Plaintiff and Class Members have suffered numerous actual and imminent injuries as a direct result of the Data Breach, including: (a) theft of their Sensitive Information; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of the Data Breach; (d) invasion of privacy; (e) emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft posed by their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) the diminution in value of their personal data; (h) the loss of value of the bargain for paying for services that required entrusting their Sensitive Information to Defendant with the mutual understanding that Defendant would safeguard the Sensitive Information against improper disclosure, misuse, and theft; and (h) the continued risk to their Sensitive

Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Sensitive Information.

20. Plaintiff seeks to remedy these harms, and to prevent their future occurrence, on behalf of themselves and all similarly situated persons whose Sensitive Information were compromised as a result of the Data Breach.

21. Accordingly, Plaintiff, on behalf of himself and other Class Members, asserts claims for negligence (Count I); negligence *per se* (Count II); breach of fiduciary duty (Count III); breach of implied contract (Count IV); and Declaratory Judgment (Count V).

PARTIES

Plaintiff Winston Fernandez

22. Plaintiff Winston Fernandez is a resident and citizen of Pennsylvania residing in Lansford, Pennsylvania in Carbon County. Mr. Fernandez received AUS's Notice of Data Breach, dated January 4, 2023, shortly after that date.

23. The letter, dated January 4, 2023, informed Plaintiff Fernandez that, following an internal investigation, Defendant had determined that certain AUS files were accessed without authorization November 28, 2022. The letter further states that a comprehensive review concluded that compromised files contained Plaintiff Fernandez's full name and Social Security number, but that AUS is unable

to confirm other specific information that may have been affected in the Data Breach.

Defendant AUS

24. Defendant AUS, Inc. is a New Jersey corporation with its principal place of business at 155 Gaither Dr., Ste. A, Mount Laurel, NJ 08054.

25. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

26. All of Plaintiff's claims stated herein are asserted against AUS and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

JURISDICTION AND VENUE

27. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one other Class Member, including Plaintiff, is a citizen of a state different from Defendant to establish minimal diversity.

28. The District of New Jersey has personal jurisdiction over Defendant named in this action because Defendant is incorporated and has its principal place

of business in this District, conducts substantial business in this District through its headquarters, offices, and affiliates, and (upon information and belief) engaged in the conduct at issue here in this judicial district.

29. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant is headquartered and has its principal place of business in this District and has caused harm to Plaintiff and Class Members through conduct in this District.

FACTUAL ALLEGATIONS

Background

30. In its Notice Letters, AUS assures its customers and employees that it takes "the privacy and security of the information entrusted to us very seriously." Further, though AUS itself does not have a publicly available website stating its Privacy Policy, its subsidiaries clearly proclaim their concern for their customers' privacy and security, and voluntarily assume the mantle of protecting their PII.

> SSRS designs, fields, manages and analyzes surveys on people's attitudes and behavior. We share your concerns about maintaining the integrity and privacy of personal information collected. We strive to conform our privacy practices to applicable laws and regulations as well as the Code of Professional Ethics and Standards of the American Association for Public Opinion Research (AAPOR).[4]
>
> Marketing Systems Group. ("MSG") is strongly committed to protecting the privacy of purchasers ("Purchasers") of its products and services.[5]

[4] https://ssrs.com/privacy-policy/ (last accessed Mar. 23, 2023)
[5] https://www.m-s-g.com/Pages/msg/privacy (last accessed Mar. 23, 2023)

> At AUS, we protect the things we really care about. That's why managing data in a safe way is top priority for us. Data protection, privacy and security are more than just rules or regulations. These areas are ingrained into our culture and are at the core of how we deliver trusted products and services. Our privacy and security programs govern how we collect, use, and manage employee, client and customer information. Everyone within our organization is responsible for demonstrating compliance when it comes to data protection, privacy and security.[6]

31. AUS also promises consumers that it will keep personal information only as long as it needs to, and that it will remove the personal data from its systems or depersonalize it in accordance with relevant law. It assures customers that it will only share their personal information as required by law, but that it is committed to maintaining customers' privacy.[7]

32. Plaintiff and the Class Members, as current and former AUS customers, and/or current and former AUS employees, relied on these expressed and implied promises and on this sophisticated entity to keep their sensitive PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Consumers, in general, demand security to safeguard their PII, especially when Social Security numbers and other sensitive PII is involved.

33. AUS had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII from involuntary disclosure to third parties.

The Data Breach

[6] https://royaltysource.com/privacy_policy.html (last accessed Mar. 23, 2023)
[7] *Id*.

34. Beginning on or about January 4, 2023, AUS notified many of its customers, current and former employees, and state Attorneys General about a widespread data breach involving sensitive PII of certain current and former customers.

35. Through an investigation, AUS determined that the unauthorized individual or individuals gained access to its systems on November 28, 2023. This exposed an estimated 3,400 individuals' PII to criminals.

36. On December 23, 2022, an investigation commissioned by AUS determined that there was unauthorized activity on AUS's network that resulted in unauthorized third-party access to and acquisition of confidential information of AUS customers, but that the full scope and specifics of the information impacted could not be determined. The Data Breach was determined to be a ransomware attack.[8]

37. The confidential information that was accessed without authorization included names along with data elements including full names and Social Security numbers.[9]

38. Upon information and belief, the PII was not encrypted prior to the data breach.

39. Upon information and belief, the cyberattack was targeted at AUS due

[8] Data Breach Notice Letter.
[9] *Id*.

to its status as complicated parent company of several subsidiaries offering business related services throughout the country, thereby collecting valuable personal and financial data from its many customers, as well as its employees.

40. Upon information and belief, the cyberattack was expressly designed to gain access to private and confidential data, including (among other things) the PII of Plaintiff and the Class Members.

41. On or about January 4, 2023, AUS sent customers (including Mr. Fernandez) and current or former employees a Data Breach Notice Letter informing the recipients of the notice that their confidential data was involved, and stating:

> We are writing to inform you that AUS, Inc. ("AUS"), the parent company of SSRS, MSG, RoyaltySource, and AUS Consultants, recently experienced a ransomware attack that may have involved some of your information described below. The information believed to be at risk from this incident includes information related to current and former employees. While we have no evidence of attempted or actual misuse of your information as a result of this incident, we are providing you with information about the incident, the measures we have taken in response, and steps you can take to help protect your information, should you feel it appropriate to do so.
>
> On November 23, 2022, AUS experienced a ransomware attack resulting in limited network disruption. Upon discovery of the incident, AUS immediately deployed all available resources ad began an investigation. AUS continues to work with I.T. staff and third-party technical experts to determine the full nature and scope of this incident. We also reported this incident to federal law enforcement. While our investigation remains ongoing, we have discovered that certain AUS current and former employee data, kept in the normal course of business, may have been subject to unauthorized access. Upon discovery, we compiled a list of potentially impacted individuals in order to provide this notification. This process was completed on December 23, 2022. Although we are unable to confirm the

> specific information that may be affected for each individual at this time, we are providing notification out of an abundance of caution.
>
> While our investigation into this incident remains ongoing, at this time the information believed to have been subject to unauthorized access may include your first and last name, in combination with your Social Security number.[10]

42. AUS admitted in the Notice of Data Breach and the letters to the Attorneys General that their systems were subjected to unauthorized access on November 28, 2023 in the course of a ransomware attack and there is no indication that the exfiltrated PII was retrieved from the cybercriminals who took it.[11]

43. AUS's offer of credit and identity monitoring services, AUS's suggestion to "remain vigilant," as well as the express warning for any "unauthorized activity" is an acknowledgment by AUS that the impacted customers are subject to an imminent threat of identity theft and financial fraud.[12]

44. In response to the Data Breach, AUS claims, it "deployed all available resources and began an investigation." AUS has since implemented more stringent security procedures internally, but there is no indication whether these steps are adequate to protect Plaintiff's and Class Members' PII going forward.

45. AUS had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep their PII confidential and to protect it from unauthorized access and disclosure.

---

[10] *Id.*
[11] *Id.*
[12] *Id.*

46. Plaintiff and Class Members provided their PII to AUS with the reasonable expectation and mutual understanding that AUS would comply with its obligations and representations to keep such information confidential and secure from unauthorized access.

47. AUS failed to uphold its obligations to Plaintiff and Members of the Class. As a result, Plaintiff and Class Members have been significantly harmed and will be at a high risk of identity theft and financial fraud for many years to come.

48. AUS did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining, causing Plaintiff's and Class Members' PII to be exposed.

Securing PII and Preventing Breaches

49. AUS could have prevented this Data Breach by properly encrypting or otherwise protecting their equipment and computer files containing PII.

50. AUS has acknowledged the sensitive and confidential nature of the PII. To be sure, collecting, maintaining, and protecting PII is vital to many of AUS's business purposes. AUS has acknowledged through conduct and statements that the misuse or inadvertent disclosure of PII can pose major privacy and financial risks to impacted individuals, and that under state law they may not disclose and must take reasonable steps to protect PII from improper release or disclosure.

The Data Breach Was a Foreseeable Risk of which Defendant Was on Notice

51. It is well known that PII, including social security numbers and financial account information in particular, is an invaluable commodity and a frequent target of hackers.

52. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.

53. Of the 1,473 recorded data breaches, 108 of them were in the banking/credit/financial industry, with the number of sensitive records being exposed exceeding 100 million. In fact, over 62% of the 164 million sensitive records exposed in data breaches in 2019 were exposed in those 108 breaches in the banking/credit/financial sector.

54. The 108 reported financial sector data breaches reported in 2019 exposed 100,621,770 sensitive records, compared to 2018 in which only 1,778,658 sensitive records were exposed in financial sector breaches.

55. Consumers place a high value not only on their PII, but also on the privacy of that data. This is because identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.

56. Consumers are particularly concerned with protecting the privacy of their financial account information and social security numbers, which are the "secret sauce" that is "as good as your DNA to hackers." There are long-term

consequences to data breach victims whose social security numbers are taken and used by hackers. Even if they know their social security numbers have been accessed, Plaintiff and Class Members cannot obtain new numbers unless they become a victim of social security number misuse. Even then, the Social Security Administration has warned that "a new number probably won't solve all [] problems … and won't guarantee … a fresh start."

57. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), AUS knew or should have known that its electronic records would be targeted by cybercriminals.

58. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack.

59. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite their own acknowledgment of its duties to keep PII private and secure, AUS failed to take appropriate steps to protect the PII of Plaintiff and the proposed Class from being compromised.

At All Relevant Times, AUS Had a Duty to Plaintiff and Class Members to Properly Secure their Private Information

60. At all relevant times, AUS had a duty to Plaintiff and Class Members to properly secure their PII, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiff and Class Members, and to promptly notify Plaintiff and Class Members when AUS became aware that their PII may have been compromised.

61. AUS's duty to use reasonable security measures arose as a result of the special relationship that existed between AUS, on the one hand, and Plaintiff and the Class Members, on the other hand. The special relationship arose because Plaintiff and the Members of the Class entrusted AUS with their PII when they purchased financial products or services from AUS.

62. AUS had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information. Accordingly, AUS breached its common law, statutory, and other duties owed to Plaintiff and Class Members.

63. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user

access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for PII;

i. Monitoring for server requests from VPNs; and

j. Monitoring for server requests from Tor exit nodes.

64. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."

65. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

66. The ramifications of AUS's failure to keep its consumers' PII secure are long- lasting and severe. Once PII is stolen, particularly Social Security and driver's license numbers, fraudulent use of that information and damage to victims

may continue for years.

The Value of Personal Identifiable Information

67. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.13 According to the Dark Web Price Index for 2021, payment card details for an account balance up to $1,000 have an average market value of $150, credit card details with an account balance up to $5,000 have an average market value of $240, stolen online banking logins with a minimum of $100 on the account have an average market value of $40, and stolen online banking logins with a minimum of $2,000 on the account have an average market value of $120.14 Criminals can also purchase access to entire company data breaches from $900 to $4,500.15

68. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of

---

[13] *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark- web-how-much-it-costs/.

[14] *Dark Web Price Index 2021*, Zachary Ignoffo, March 8, 2021, available at: https://www.privacyaffairs.com/dark-web-price-index-2021/

[15] *In the Dark*, VPNOverview, 2019, available at: https://vpnoverview.com/privacy/anonymous- browsing/in-the-dark/.

fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[16]

69. A new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[17]

70. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[18]

---

[16] Social Security Administration, Identity *Theft and Your Social Security Number*, available at: https://www.ssa.gov/pubs/EN-05-10064.pdf.
[17] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has- millions-worrying-about-identity-theft.
[18] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015),

71. PII can be used to distinguish, identify, or trace an individual's identity, such as their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[19]

72. Given the nature of the Data Breach, it is foreseeable that the compromised PII can be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Class Members' PII can easily obtain Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

73. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because, there, victims can cancel or close credit and debit card accounts.[25] The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

74. To date, AUS has offered its consumers only one year of identity monitoring service. The offered services are inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the

---

http://www.itworld.com/article/2880960/anthem- hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[19] See OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1.

PII at issue here.

75. The injuries to Plaintiff and Class Members were directly and proximately caused by AUS's failure to implement or maintain adequate data security measures for its current and former customers.

AUS Failed to Comply with FTC Guidelines

76. Federal and State governments have likewise established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[20]

77. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[2127] The guidelines note businesses should protect the personal consumer and consumer information that they keep, as well as properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their

[20] Federal Trade Commission, *Start With Security*, available at: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

[21] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at: https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information- guide-business

network's vulnerabilities; and implement policies to correct security problems.

78. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[22]

79. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only

[22] FTC, Start With Security, supra note 28.

trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

80. The FTC has brought enforcement actions against businesses for failing to protect consumer and consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

81. Because Class Members entrusted AUS with their PII, AUS had, and has, a duty to the Class Members to keep their PII secure.

82. Plaintiff and the other Class Members reasonably expected that when they provide PII to AUS, AUS would safeguard their PII.

83. AUS was at all times fully aware of its obligation to protect the personal and financial data of consumers, including Plaintiff and members of the

Classes. AUS was also aware of the significant repercussions if it failed to do so.

84. AUS's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—including Plaintiff's and Class Members' names and Social Security numbers — constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

Plaintiff and Class Members Have Suffered Concrete Injury As A Result Of Defendant's Inadequate Security And The Data Breach It Allowed

85. Plaintiff and Class Members reasonably expected that Defendant would provide adequate security protections for their PII, and Class Members provided Defendant with sensitive personal information, including their Social Security numbers.

86. Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Defendant for its service, Plaintiff and other reasonable consumers understood and expected that they were paying for services and data security, when in fact Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected. As such, Plaintiff and the Class Members suffered pecuniary injury.

87. Cybercriminals capture PII to exploit it; the Class Members are now, and for the rest of their lives will be, at a heightened risk of identity theft. Plaintiff has also incurred (and will continue to incur) damages in the form of, inter alia, loss

of privacy and costs of engaging adequate credit monitoring and identity theft protection services.

88. The cybercriminals who obtained the Class Members' PII may exploit the information they obtained by selling the data in so-called "dark markets." Having obtained these names, addresses, Social Security numbers, and other PII, cybercriminals can pair the data with other available information to commit a broad range of fraud in a Class Member's name, including but not limited to:

a. obtaining employment;

b. obtaining a loan;

c. applying for credit cards or spending money;

d. filing false tax returns;

e. stealing Social Security and other government benefits; and

f. applying for a driver's license, birth certificate, or other public document.

89. In addition, if a Class Member's Social Security number is used to create false identification for someone who commits a crime, the Class Member may become entangled in the criminal justice system, impairing the person's ability to gain employment or obtain a loan.

90. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiff and the other Class Members have been deprived of the value of their PII, for which there is a well-

established national and international market.

91. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for an information breach to be detected.[23]

92. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff and the other Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud.[24] Indeed, "[t]he level of risk is growing for anyone whose information is stolen in a data breach."[25] Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers at a substantial risk of fraud."[26] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that have not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class Members' PII will do so at a

---

[23] *Id.*

[24] *Data Breach Victims More Likely To Suffer Identity Fraud*, INSURANCE INFORMATION INSTITUTE BLOG (February 23, 2012), http://www.iii.org/insuranceindustryblog/?p=267.

[25] Susan Ladika, *Study: Data Breaches Pose A Greater Risk*, CREDITCARDS.COM (July 23, 2014), http://www.creditcards.com/credit-card-news/data-breach-id-theft-risk-increase-study- 1282.php.

[26] THE CONSUMER DATA INSECURITY REPORT: EXAMINING THE DATA BREACH- IDENTITY FRAUD PARADIGM IN FOUR MAJOR METROPOLITAN AREAS, (available at https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf).

later date or re-sell it.

93. As a result of the Data Breach, Plaintiff and Class Members have already suffered damages.

94. Since the Data Breath, Defendant has represented to the Class Members that a "comprehensive review" reveals that customers' individual files were accessed. Regardless, EmiSoft, an award-winning malware-protection software company, states that "[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence, especially during the preliminary stages of the investigation."[27][33]

95. In this case, according to AUS, cybercriminals had access to Plaintiff and Class Members' data on at least November 28, 2022.

96. However, even if AUS has not found evidence of data being exfiltrated and viewed, this would not be an assurance that the data was not accessed, acquired, and stolen. Indeed, the likelihood that cybercriminals stole the data covertly is significant, likely, and concerning.

Plaintiff Winston Fernandez's Experience

97. In or about 2021, Plaintiff Winston Fernandez was employed by an AUS, Inc. subsidiary, SSRS. As a condition to his employment, AUS required

[27] EmiSoft Malware Lab, The chance of data being stolen in a ransomware attack is greater than one in ten (EMISOFT BLOG July 13, 2020), https://blog.emsisoft.com/en/36569/the-chance-of- data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/.

Plaintiff to supply, and he provided, AUS with his PII, including but not limited to his name, address, date of birth, Social Security number, telephone number and email address. Upon information and belief, at the time of engaging the services, Plaintiff's PII was entered into AUS's systems.

98. Plaintiff Fernandez greatly values his privacy and Sensitive Information. Plaintiff has taken reasonable steps to maintain the confidentiality of his PII, and he has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

99. Plaintiff Fernandez expected and reasonably relied upon Defendant as part of its services to provide adequate data security to protect the PII that he entrusted to Defendant. If Mr. Fernandez had known that AUS would not adequately protect his PII, he would not have allowed AUS access to this sensitive and private information and would not have engaged in business with Defendant.

100. Upon information and belief, Plaintiff's PII was targeted, accessed, and downloaded and stolen by the third-party criminal actors in the Data Breach.

101. As a result of the Data Breach, Plaintiff Fernandez faces a substantial risk of imminent identity and financial fraud and theft—both now and for years to come. Mr. Fernandez has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen PII, especially his Social Security number, being placed in the hands of unauthorized third-parties and possibly criminals.

102. Indeed, Mr. Fernandez has already fallen prey to criminals with access to his Social Security number and name, as just three months after the Data Breach purportedly occurred, Mr. Fernandez received notice that a third party attempted to gain access to his Fifth Third Bank account. This instance of attempted identity theft is directly attributable to the Data Breach and is potentially the first of many such fraudulent actions or attempts that Mr. Fernandez will have to navigate moving forward.

103. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Fernandez faces, Defendant provided Plaintiff Fernandez a two-year subscription to a credit monitoring service. Because Mr. Fernandez is still grappling with the aftermath of the Data Breach and is understandably skeptical of Defendant's offers at this stage, he has not enrolled in the credit monitoring services offered.

104. Mr. Fernandez suffered actual injury in the form of damages and diminution in the value of his PII—a form of intangible property that he entrusted to AUS for the purpose of providing him services, which was compromised in and as a result of the Data Breach.

105. Furthermore, Mr. Fernandez suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy, especially his Social Security number.

106. Further, Mr. Fernandez has suffered actual injury in the form of instances of actual identity theft, beginning with the notification he received from Fifth Third Bank.

107. Moving forward, Mr. Fernandez has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in AUS's possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

108. Plaintiff brings this nationwide class action on behalf of himself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

109. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> **All persons who reside in the United States who received or were otherwise sent the AUS notice that their data was potentially compromised due to the Data Breach (the "Class)")**

110. Excluded from the Class are the following individuals and/or entities: AUS and AUS's parents, subsidiaries, affiliates, officers and directors, and any entity in which AUS has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as

well as their immediate family members.

111. Plaintiff reserves the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

112. Numerosity, Fed R. Civ. P. 23(a)(1): Classes are so numerous that joinder of all members is impracticable. AUS has identified over 3,100 consumers whose PII may have been improperly accessed in the Data Breach, and the Classes are apparently identifiable within AUS's records.

113. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact

common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent AUS had a duty to protect the PII of Plaintiff and Class Members;

b. Whether AUS had respective duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

c. Whether AUS had respective duties not to use the PII of Plaintiff and Class Members for non-business purposes;

d. Whether AUS expressly or impliedly promised to safeguard the PII of Plaintiff and Class Members.

e. Whether AUS failed to adequately safeguard the PII of Plaintiff and Class Members;

f. Whether and when AUS actually learned of the Data Breach;

g. Whether AUS adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

h. Whether AUS violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

i. Whether AUS failed to design, implement and maintain reasonable security procedures and practices in compliance with industry standards and appropriate to the nature and scope of the information compromised in the Data Breach;

j. Whether AUS adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

k. Whether AUS engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members;

l. Whether Plaintiff and Class Members are entitled to actual, damages, statutory damages, and/or punitive damages as a result of AUS's wrongful conduct;

m. Whether Plaintiff and Class Members are entitled to restitution as a result of AUS's wrongful conduct;

n. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach;

114. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to AUS's misfeasance.

115. Policies Generally Applicable to the Class: This class action is also appropriate for certification because AUS has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members, and making final injunctive relief appropriate with respect to the Class

as a whole. AUS's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on AUS's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

116. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages he has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex consumer class action litigation, and Plaintiff intend to prosecute this action vigorously.

117. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like AUS. Further, even for those Class Members

who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

118. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because AUS would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

119. The litigation of the claims brought herein is manageable. AUS's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

120. Adequate notice can be given to Class Members directly using information maintained in AUS's records.

121. Unless a Class-wide injunction is issued, AUS may continue in its

failure to properly secure the PII of Class Members, AUS may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and AUS may continue to act unlawfully as set forth in this Complaint.

122. Further, AUS has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

123. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether AUS owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether AUS breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether AUS failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between AUS on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. Whether AUS breached the implied contract;

f. Whether AUS adequately, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether AUS failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach

h. Whether AUS engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members; and,

i. Whether Class Members are entitled to actual damages, statutory damages, injunctive relief, and/or punitive damages as a result of AUS's wrongful conduct.

COUNT I
Negligence
(On behalf of Plaintiffs and the Nationwide Class)

124. Plaintiff restates and realleges all of the foregoing Paragraphs 1 through 123 as if fully set forth herein.

125. As a condition of their using the services of AUS, consumers were obligated to provide AUS with certain PII, including their name, Social Security number.

126. Plaintiff and Class Members entrusted their PII to AUS on the premise and with the understanding that AUS would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

127. AUS has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

128. AUS knew or reasonably should have known that the failure to

exercise due care in the collecting, storing, and using of their consumers' PII involved an unreasonable risk of harm to Plaintiff and Class Members, even if the harm occurred through the criminal acts of a third party.

129. AUS had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing AUS's security protocols to ensure that Plaintiff's and Class Members' information in AUS's possession was adequately secured and protected.

130. AUS also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and Class Members' PII.

131. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class Members was reasonably foreseeable, particularly in light of AUS's inadequate security practices.

132. Plaintiff and the Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. AUS knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on AUS's systems.

133. AUS's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. AUS's misconduct included, but was not limited to, its failure to

take the steps and opportunities to prevent the Data Breach as set forth herein. AUS's misconduct also included its decisions not to comply with industry standards for the safekeeping of Plaintiff's and Class Members' PII, including basic encryption techniques freely available to AUS.

134. Plaintiff and the Class Members had no ability to protect their PII that was in, and possibly remains in, AUS's possession.

135. AUS was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

136. AUS had and continues to have a duty to adequately disclose that the PII of Plaintiff and Class Members within AUS's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

137. AUS had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and Class Members.

138. AUS has admitted that the PII of Plaintiff and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

139. AUS, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to implement industry protocols

and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and Class Members during the time the PII was within AUS's possession or control.

140. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for

Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

141. These foregoing frameworks are existing and applicable industry standards in the financial services industry, and Defendant failed to comply with these accepted standards thereby opening the door to the cyber incident and causing the data breach.

142. AUS improperly and inadequately safeguarded the PII of Plaintiff and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

143. AUS failed to heed industry warnings and alerts to provide adequate safeguards to protect consumers' PII in the face of increased risk of theft.

144. AUS, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its consumers' PII.

145. AUS, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and Class Members the existence and scope of the Data Breach.

146. But for AUS's wrongful and negligent breach of duties owed to Plaintiff and Class Members, the PII of Plaintiff and Class Members would not have been compromised.

147. There is a close causal connection between AUS's failure to implement security measures to protect the PII of Plaintiff and Class Members and the harm suffered or risk of imminent harm suffered by Plaintiff and the Class. Plaintiff's and Class Members' PII was lost and accessed as the proximate result of AUS's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

148. As a direct and proximate result of AUS's negligence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover

from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in AUS's possession and is subject to further unauthorized disclosures so long as AUS fails to undertake appropriate and adequate measures to protect the PII of consumers in their continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (ix) the diminished value of AUS's goods and services they received.

149. As a direct and proximate result of AUS's negligence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

150. Additionally, as a direct and proximate result of AUS's negligence and negligence per se, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their PII, which remain in AUS's possession and is subject to further unauthorized disclosures so long as AUS fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

COUNT II
Negligence *Per Se*
(On behalf of Plaintiffs and the Nationwide Class)

151. Plaintiff restates and realleges the foregoing Paragraphs 1 through 150

as if fully set forth herein.

152. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security to safeguard the PII of Plaintiff and Class Members.

153. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as AUS, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of AUS's duty in this regard.

154. Pursuant to the Gramm-Leach-Bliley Act, Defendant had a duty to protect the security and confidentiality of Plaintiff's and Class Members' PII. *See* 15 U.S.C. § 6801.

155. Pursuant to the Fair Credit Reporting Act ("FCRA"), Defendant had a duty to adopt, implement, and maintain adequate procedures to protect the security and confidentiality of Plaintiff's and Class Members' PII. *See* 15 U.S.C. § 1681(b).

156. Defendant solicited, gathered, and stored PII of Plaintiff and the Class Members to facilitate transactions which affect commerce.

157. Defendant violated the FTC Act (and similar state statutes), FCRA, and the Graham-Leach-Bliley Act by failing to use reasonable measures to protect PII of Plaintiff and Class Members and not complying with applicable industry standards, as described herein. Defendant's conduct was particularly unreasonable

given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

158. Defendant's violation of the FTC Act (and similar state statutes) as well as its violations of the Graham-Leach-Bliley Act constitutes negligence *per se.*

159. Plaintiff and the Class Members are within the class of persons that the FTC Act and the Graham-Leach-Bliley Act were intended to protect.

160. The harm that occurred as a result of the breach is the type of harm the FTC Act (and similar state statutes), as well as the Graham-Leach-Bliley Act were intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures caused the same harm as that suffered by Plaintiff and the Class Members.

161. As a direct and proximate result of Defendant's negligence *per se,* Plaintiff and Class Members have suffered, and continue to suffer, damages arising from the breach as described herein and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

162. As a direct and proximate result of Defendant's negligence *per se* and the data breach, Plaintiff and members of the proposed Class have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiff and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure,

theft, and unauthorized use of Plaintiff's and Class Members' PII; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their PII; (g) the diminution in the value of the services bargained for as Plaintiff and Class Members were deprived of the data protection and security that Defendant promised when Plaintiff and the proposed class entrusted Defendant with their PII; and (h) the continued and substantial risk to Plaintiff and Class Members PII, which remains in the Defendant's possession of Defendant with in-adequate measures to protect Plaintiff's and Class Members' PII.

COUNT III
Breach of Fiduciary Duty
(On behalf of Plaintiffs and the Nationwide Class)

163. Plaintiff restates and realleges the foregoing Paragraphs 1 through 162 as if fully set forth herein.

164. In providing their Sensitive Information to Defendant, Plaintiffs and Class Members justifiably placed a special confidence in Defendant to act in good faith and with due regard to interests of Plaintiff and Class Members to safeguard and keep confidential that Sensitive Information.

165. Defendant accepted the special confidence Plaintiffs and Class

Members placed in it, as evidenced by its assertion that it is "committed to protecting the privacy of [Plaintiff's] personal information" as included in the Data Breach notification letters.

166. In light of the special relationship between Defendant and Plaintiff and Class Members, whereby Defendant became a guardian of Plaintiff's and Class Members' Sensitive Information, Defendant became a fiduciary by its undertaking and guardianship of the Sensitive Information, to act primarily for the benefit of its customers, including Plaintiff and Class Members for the safeguarding of Plaintiff' and Class Members' Sensitive Information.

167. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of its customer's relationship, in particular, to keep secure the Sensitive Information of its customers.

168. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to protect the integrity of the systems containing Plaintiff's and Class Members' Sensitive Information.

169. Defendant breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Sensitive Information.

170. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the compromise,

publication, and/or theft of their Private Information; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Sensitive Information; (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Cyber-Attack and Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their Sensitive Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Sensitive Information in its continued possession; (f) future costs in terms of time, effort, and money that will be expended as result of the Cyber-Attack and Data Breach for the remainder of the lives of Plaintiff and Class Members; and (g) the diminished value of Defendant's services they received.

171. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT IV
Breach of Implied Contract
(On behalf of Plaintiffs and the Nationwide Class)

172. Plaintiff restates and realleges the foregoing Paragraphs 1 through 171

as if fully set forth herein.

173. As a condition of receiving services, Defendant required Plaintiff and Class Members to provide their PII, including names and Social Security numbers.

174. Defendant solicited and invited Plaintiff and Class Members to provide their Private Information as part of Defendant's regular business practices.

175. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant. Defendant accepted the PII, and there was a meeting of the minds that Defendant would secure, protect, and keep the PII confidential.

176. Plaintiff fully performed his obligations under the implied contracts with Defendant.

177. Plaintiff would not have entered into transactions with AUS if Plaintiff had known AUS would not protect their PII.

178. When AUS required and accepted the PII from Plaintiff and the Class, it implied its assent to protect the information sufficiently.

179. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their PII, and by failing to provide timely and accurate notice to them that their PII was compromised as a result of the Data Breach.

180. Plaintiff and Class Members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to

obtain adequate data security. Defendant failed to do so.

181. As a direct and proximate result of Defendant's above-described breach of implied contract, have suffered and will suffer injury, including but not limited to: (a) actual identity theft;

(b) the loss of the opportunity how their PII is used; (c) the compromise, publication, and/or theft of their PII; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (e) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (f) costs associated with placing freezes on credit reports; (g) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of consumers and former consumers in its continued possession; (h) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (i) the diminished value of AUS's goods and services they received.

182. Plaintiff and Class Members are entitled to compensatory,

consequential, and nominal damages suffered as a result of the Data Breach, including the loss of the benefit of the bargain.

183. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (a) strengthen its data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) immediately provide adequate credit monitoring to all Class Members.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all Class Members, requests judgment against the AUS and that the Court grant the following:

A. For an Order certifying the Nationwide Class and appointing Plaintiff and their Counsel to represent the certified Class;

B. For equitable relief enjoining AUS from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and the Class Members' PII, and from refusing to issue prompt, complete, any accurate disclosures to the Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting AUS from engaging in the wrongful and unlawful acts described herein;

ii. requiring AUS to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring AUS to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless AUS can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring AUS to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff and Class Members' personal identifying information;

v. prohibiting AUS from maintaining Plaintiff's and Class Members' personal identifying information on a cloud-based database;

vi. requiring AUS to engage independent third-party security auditors/penetration testers as well as internal security personnel

to conduct testing, including simulated attacks, penetration tests, and audits on AUS's systems on a periodic basis, and ordering AUS to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring AUS to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring AUS to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring AUS to segment data by, among other things, creating firewalls and access controls so that if one area of AUS's network is compromised, hackers cannot gain access to other portions of AUS's systems;

x. requiring AUS to conduct regular database scanning and securing checks;

xi. requiring AUS to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of

Plaintiff and Class Members;

xii. requiring AUS to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring AUS to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with AUS's policies, programs, and systems for protecting personal identifying information;

xiv. requiring AUS to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor AUS's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring AUS to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring AUS to implement logging and monitoring programs sufficient to track traffic to and from AUS's servers; and

xvii. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate AUS's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of punitive damages;

F. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. For prejudgment interest on all amounts awarded; and

H. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Dated: March 24, 2023

Respectfully Submitted,
By: /s/ *Victoria Maniatis*

Victoria Maniatis
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
100 Garden City Plaza, Suite 500
Garden City, NY 11530
Tel: 516-741-5600
vmaniatis@milberg.com

Terence R. Coates*
MARKOVITS STOCK & DEMARCO, LLC
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com

David K. Lietz*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Avenue NW
Washington, D.C. 20015-2052
Phone: (866) 252-0878
Facsimile: (202) 686-2877
dlietz@milberg.com

Counsel for Plaintiff and Putative Class Members

**PRO HAC VICE FORTHCOMING*

EXHIBIT A

AUS

January 04, 2023

[redacted]

Dear Winston M Cuevas Fernandez:

We are writing to inform you that AUS, Inc. ("AUS"), the parent company of SSRS, MSG, RoyaltySource and AUS Consultants, recently experienced a ransomware attack that may have involved some of your information described below. The information believed to be at risk from this incident includes information related to current and former employees. While we have no evidence of attempted or actual misuse of your information as a result of this incident, we are providing you with information about the incident, the measures we have taken in response, and steps you can take to help protect your information, should you feel it appropriate to do so.

What Happened: On November 28, 2022, AUS experienced a ransomware attack resulting in limited network disruption. Upon discovery of the incident, AUS immediately deployed all available resources and began an investigation. AUS continues to work with I.T. staff and third-party technical experts to determine the full nature and scope of this incident. We also reported this incident to federal law enforcement. While our investigation remains ongoing, we have discovered that certain AUS current and former employee data, kept in the normal course of business, may have been subject to unauthorized access. Upon discovery, we compiled a list of potentially impacted individuals in order to provide this notification. This process was completed on December 23, 2022. Although we are unable to confirm the specific information that may be affected for each individual at this time, we are providing notification out of an abundance of caution.

What Information Was Involved: While our investigation into this incident remains ongoing, at this time the information believed to have been subject to unauthorized access may include your first and last name, in combination with your Social Security number.

What We Are Doing: In addition to engaging third-party experts and undergoing a thorough forensic investigation, AUS has taken a number of steps to remediate the incident, including a forced password reset enterprise-wide and the implementation of multi-factor authentication across the company. Out of an abundance of caution, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. Due to privacy laws, we cannot activate these services for you directly. Additional information regarding how to activate the complimentary identity monitoring service is enclosed. We have also provided additional information about steps you can take to help protect yourself against fraud and identity theft.

What You Can Do: We recommend that you remain vigilant in regularly reviewing and monitoring all of your accou statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious unusual activity on your accounts, please promptly contact your financial institution or company. Additionally, you ctivate the complimentary identity monitoring service we are making available to you. You can also review the enclo Steps You Can Take to Help Protect Your Information" for additional resources.